CLAIMS

1. A real-time reference monitor software product comprising, on a machine-readable medium, a sequence of instructions defining:

a storage area where real-time state information is stored and from which the state information is restored;

a plurality of rules defining allowable activity based on a pattern of activity; and

plural interceptors identifying and governing the activity based on an application of the rules to the activity.

2. The software product of claim 1, further comprising:

a process which correlates the state information across different ones of the plural interceptors.

3. The software product of claim 2, wherein at least one of the plural interceptors is a pre-existing element of a conventional computer operating system.

4. The software product of claim 2, wherein the process which correlates the state information further comprises:

a rule which defines permissible resource references in view of activity identified by the interceptors and the state information; and

a rule interpreter which applies the rule to the activity identified and the state information.

5. The software product of claim 4, wherein the rule can be modified without restarting the real-time reference monitor.

6. The software product of claim 5, wherein the storage area has contents which are preserved when the rule is modified.

7. The software product of claim 1, wherein the plural reference interceptors correspond to more than one resource type and wherein the storage area is a single storage area.

8. The software product of claim 1, further comprising:

an application program interface that can send messages to application programs on the same system.

9. The software product of claim 8, further comprising:

an application program interface that can send messages to application programs on other systems.

10. The software product of claim 1, wherein the plural reference interceptors monitor two or more of file access, registry access, network access, object access, system call access, keyboard access, external inputs and user input.

11. A computer-implemented reference monitor, comprising:

a monitoring process, executing on a computer, which detects plural defined events and generate event messages;

a storage device, on the computer, in which is stored information related to the event messages generated by the monitoring process; and

a rule interpreting process, executing on the computer, which responds to characteristics of an event message the information stored in the storage device and a set of rules by modifying operation of the computer.

12. The computer-implemented reference monitor of claim 11, wherein the set of rules is modified in response to the information stored in the storage device.

13. The computer-implemented reference monitor of claim 12, wherein the set of rules is modified and wherein the information stored in the storage device is preserved when the set of rules is modified.

14. The computer-implemented reference monitor of claim 11, further comprising:

an external event message generating process executing on another computer, wherein the external event message generating process communicates event messages to the rule interpreting process.

15. A method of implementing a processing policy on a computer, comprising:

detecting first and second events, each having one of a plurality of defined event types;

generating first and second event messages, each containing information about a corresponding one of the first and second events;

storing the information about the first event; and

enforcing the policy responsive to the stored information about the first event and the information about the second event.

16. The method of claim 15, further comprising:

applying one of a set of rules to the stored information about the first event and the information about the second event to determine the nature of enforcing the policy.

17. The method of claim 16, further comprising:

executing an operating system on the computer;

changing the set of rules without restarting the operating system and without losing the stored information.

18. The method of claim 17, further comprising:

changing the set of rules without interrupting the detecting, generating, storing and enforcing.